Information Assurance Protocols: Efficiency Analysis and Implementation for Secure Communication

Boris S. Verkhovsky
Computer Science Department, New Jersey Institute of Technology
verb@homer.njit.edu

Abstract: *Two major issues are considered in this paper*: *security of communication and reliability of connection. The paper demonstrates how to interlink both the security requirement and communication assurance into one algorithmic procedure. Several reliability protocols are described and their characteristics (probabilities of failure, bandwidth requirement per block of transmitted ciphertext and complexity of recovery) are analyzed and compared.*

Key words: reliability protocol; information assurance; public-key cryptography; bandwidth requirement

1. Introduction

In modern communication networks, which transmit highly-sensitive commercial, financial, legal, military and other information, two major requirements must be met: reliability of connection and security of delivery. Both requirements have been well analyzed in communication theory [1]-[3], [6], and thoroughly developed in cryptography [5, 7, 8]. The reliability of connection and information transmission is assured by communication protocols that provide an elaborate system of acknowledgements (ACKs, for short) [4], [9]. In these protocols a sender repeatedly transmits a block of information (packet or cell) to a receiver until the intended receiver sends an ACK. In addition, prior to transmission each block of information is cryptographically protected by the sender for security reasons.

The implementation of these two algorithms of information processing requires extra time and additional bandwidth. These are major drawbacks if speedy delivery is essential. Information transmission in a military environment and in financial exchanges between brokers and customers are examples in which delay is a sensitive issue, [9]. Another example is secure lines of a voice communication over Internet (VoIP): in these lines reliability, security and real-time communication are paramount requirements [4].

This paper illustrates how to interlink the communication assurance and security requirement into algorithmic protocols. An analysis of computational complexity of such a tandem and trade-off between degree of crypto-immunity and bandwidth requirements of its implementation is provided.

In the paper [11] it is demonstrated how to use complexity of cubic root extraction modulo composite $n=pq$ for encryption and decryption.

2. Problem statement

Two major concerns are addressed in the paper:
1). Protection of information transmitted over open channels/links from a potential intruder (security consideration);
2). Assurance of the transmitted information, i.e., how to guarantee that this information is successfully delivered to an intended receiver with required probability (reliability consideration) [3].
Security protection: a generic cryptographic procedure is described.
Reliability mechanism: redundancy protocols are considered and analyzed.

Definition 1: A protocol, handling r channels/links over which h units of information $\{u_1, u_2, ..., u_h\}$ are transmitted, is called $P(r, h)$-protocol. Here $1 \le h \le r$.

If every channel is absolutely reliable, (i.e., if its probability of failure $f=0$), then the most efficient transmission protocol is $P(1, 1)$-protocol, i.e., where redundancy is absent. However, in most of system and/or human communication a certain degree of redundancy is necessary, since there is always a chance of communication failure, (i.e., the probability of successful transmission is less than 100%). Although a redundancy does not provide absolute assurance of information delivery, yet, if properly handled, it substantially increases probability $S_{r,h}$ of successful transmission if $P(r, h)$-protocol is used for communication.

Definition 2: If in $P(r, h)$-protocol all h blocks of information are received and recovered by the intended receiver, then such transmission is called successful.

Since modern communication is an expensive and complex process, (it requires financial resources, bandwidth and time), it should be designed to satisfy all technical and other requirements and to optimize usage of these resources. Several

Received September 23, 2008
Dynamic Publishers, Inc

1554-1010 $03.50 ©

algorithms are described in the paper, and their performance is analyzed and compared.

3. Transmission assuring protocols

3.1. *P*(3,2)-protocol

Consider a *pair* of plaintext blocks a and b represented as integers on the interval $2 \le a \le n-2;\ 2 \le b \le n-2$.
Suppose that

$$\{u, v, w\} := \{E(a+b), E(2a+b), E(a-b)\} \bmod n \tag{3.1}$$

are *three* corresponding ciphertext blocks. Here E is an encryption algorithm {RSA, Rabin, ElGamal, elliptic-curve cryptography or public key cryptography based on extraction of cubic roots-see references [5], [7], [8]; [10] and [11]}. In (3.1) and further in the paper modulo reduction is applied to every component.
It is clear that if any *two* out of *three* components in (3.1) are successfully transmitted to a receiver (*Bob*), then after decryption *Bob* is able to recover the plaintext blocks a and b. For example, if the values

$$u = E(a+b) \text{ and } v = E(2a+b) \tag{3.2}$$

are successfully transmitted, then *Bob* after decryption of u and v finds $a+b$ and $2a+b$, and finally determines a and b. Bob analogously proceeds if he receives either (v and w) or (u and w).
However, the *P*(3,2)-protocol fails if less than *two* ciphertext blocks are successfully transmitted. Hence the probability of failure in the *P*(3,2)-protocol is equal

$$F_{3,2} = f^3 + 3f^2(1-f) = 3f^2 - 2f^3. \tag{3.3}$$

If $f \ll 1$, then (3.3) implies that

$$F_{3,2} = 3f^2 - o_1(f). \tag{3.4}$$

Here $o_1(f) \ll 3f^2$, i.e. the last term $o_1(f) := 2f^3$ in (3.3) is substantially smaller then the former one.

3.2. *P*(4,2)-protocol

Consider a combination of *four* integers:

$$\{u_1, u_2, u_3, u_4\} := E\{a+b, 2a+b, a-b, a-2b\} \bmod n. \tag{3.5}$$

In this protocol a communication is successful if at least *two* $\{u_i, u_j\}$ out of *four* values $\{u_1, u_2, u_3, u_4\}$ in (3.5) are successfully transmitted. And it fails if less than *two* out of *four* ciphertext blocks in (3.5) are successfully delivered to the receiver. Thus, if $f \ll 1$, then

$$F_{4,2} = f^4 + 4f^3(1-f) = 4f^3 + o_2(f). \tag{3.6}$$

3.3. *P*(6,3)-protocol

Let {*a, b, c*} be *three* consecutive blocks of a plaintext.
Consider *six* combinations of these blocks:

$$\{a,\ a-b,\ b-c,\ c,\ a+b+c,\ a+2b+c\}. \tag{3.7}$$

It is easy to verify that every subset consisting of *three* elements in (3.7) is *linearly independent*, which means that none of its elements can be expressed as a linear combination of other elements. Otherwise the original message {*a, b, c*} is not recoverable. Let's consider *six* corresponding cipher-blocks:

$$u_1 := E(a) \bmod n;\ \ u_2 := E(a-b) \bmod n; \tag{3.8}$$

$$u_3 := E(b-c) \bmod n;\ \ u_4 := E(c) \bmod n; \tag{3.9}$$

$$u_5 := E(a+b+c) \bmod n;\ u_6 := E(a+2b+c) \bmod n. \tag{3.10}$$

In this protocol the transmission is successful if at least *three* $\{u_i, u_j, u_k\}$ out of *six* values $\{u_1, u_2, u_3, u_4, u_5, u_6\}$ in (3.8)-(3.10) are successfully delivered to the receiver. Otherwise, the *P*(6,3)-protocol fails.

3.4. Reliability analysis of *P*(6,3) protocol

The overall probability of failure is equal

$$F_{6,3} := f^6 + 6f^5(1-f) + 15f^4(1-f)^2 = 15f^4 + o_3(f) \tag{3.11}$$

If $f \ll 1$, then (3.11) implies that

$$F_{6,3} = 15f^4 + o_3(f). \tag{3.12}$$

Here the term $o_3(f)$ is substantially smaller than $15f^4$.

3.5. *P*(6,4)-protocol

Suppose that {*a, b, c, d*} are *four* consecutive blocks of a plaintext. Consider *six* combinations of these blocks:

$$\left\{ \begin{matrix} a+c,\ b+d,\ a-b,\ c-d, \\ a+b-c+d,\ a+b+c-d \end{matrix} \right\}. \tag{3.13}$$

Notice that every subset consisting of *four* elements in (3.13) is *linearly independent*. Otherwise the original message {*a, b, c, d*} is not recoverable.
Let's consider *six* corresponding cipher-blocks:

$$u_1 := E(a+c) \bmod n;\ \ u_2 := E(b+d) \bmod n; \tag{3.14}$$

$$u_3 := E(a-b) \bmod n;\ \ u_4 := E(c-d) \bmod n; \tag{3.15}$$

$$u_5 := E(a+b-c+d) \bmod n;\ u_6 := E(a+b+c-d) \bmod n \tag{3.16}$$

In this protocol the transmission is successful if at least any *four* out of *six* values $\{u_1, u_2, u_3, u_4, u_5, u_6\}$ in (3.14)-(3.16) are successfully delivered to the receiver.
Otherwise, the *P*(6,4)-protocol fails.
Hence

$$F_{6,4} := f^6 + 6f^5(1-f) + 15f^4(1-f)^2 + 20f^3(1-f)^3. \tag{3.17}$$

Analogously, if the probability of failure f is substantially smaller than *one*, then

Received September 23, 2008
1554-1010 $03.50 © Dynamic Publishers, Inc

$$F_{6,4} := 20f^3 + o_4(f). \quad (3.18)$$

3.6. *P*(3,2)-protocol revisited

The combination (3.1) is only one of many possibilities to design this protocol. Here is an example of a non-linear case:

$$\{u, v, w\} := \left\{E(a+b), E(a-b), E\left(a^2-b^2\right)\right\} \bmod n. \quad (3.19)$$

The original plaintext blocks are also recoverable. However, if either (*u* and *w*) or (*v* and *w*) are successfully transmitted, then the recovery of *a* and *b* requires one operation of modular multiplicative inverse and one modular multiplication. Indeed, suppose Bob received *u* and *w* and after decryption found $G:=(a+b) \bmod n$ and $H := \left(a^2-b^2\right) \bmod n$.

In order to recover the original blocks *a* and *b* Bob needs to compute

$$G^{-1} := (a+b)^{-1} \bmod n. \quad (3.20)$$

Then after one modular multiplication Bob finds

$$a - b \equiv HG^{-1} \bmod n. \quad (3.21)$$

The operation (3.20) has time complexity O(log*n*) [12], [13]; besides multiplication of large integers has quadratic bit-wise complexity while additions and subtractions have linear bit-wise complexity. It is obvious that the implementation of *P*(3,2)-protocol described in (3.19) is more time demanding than the protocol implementation provided in (3.1).

In conclusion, it is worth to mention the following two additional facts:

1). *P*(3,2) is the simplest of all information assuring protocols, especially as it is described in (3.1);

2) Although $F_{3,2}$ is *three* times larger than $F_{2,1}$, in case, if $B_{3,2}<t$, the *P*(3,2)-protocol has an advantage over *P*(2,1). Indeed, the corresponding bandwidth requirements are $B_{3,2}=1.5$ and $B_{2,1}=2$. Hence, *P*(2,1) requires 33.3% more bandwidth than *P*(3,2)-protocol.

4. Properties of *P*(*r*,*h*)-protocol

4.1. Reliability analysis

Suppose that *f* is a probability of link failure. Then probability $S_{r.h}$ of successful transmission for *P*(*r*,*h*)-protocol equals

$$S_{r,h} := \sum_{k=0}^{r-h} \binom{r}{r-k} (1-f)^{r-k} f^k = 1 - F_{r,h}, \quad (4.1)$$

where $F_{r,h}$ is the probability of link failure

$$F_{r,h} := \sum_{k=0}^{h-1} \binom{r}{k} (1-f)^k f^{r-k}. \quad (4.2)$$

If $f<<1$, then

$$F_{r,h} := \binom{r}{h-1} f^{r-(h-1)} + o(f); \quad (4.3)$$

where the term $o(f)$ is substantially smaller in comparison with the first summand in (4.3).

4.2. Monotonic properties of $F_{r,h}$

Proposition1: If $f < 1 - \frac{h-1}{r+1}$,

then $$F_{r+1,h} < F_{r,h}. \quad (4.4)$$

In other words, the probability of failure is a *decreasing* function of *r*. Indeed,

$$F_{r+1,h} / F_{r,h} = \binom{r+1}{h-1} f^{r+1-(h-1)} / \binom{r}{h-1} f^{r-(h-1)} = (r+1) f / (r+2-h). \quad (4.5)$$

Proposition2: If $f < \frac{r+1}{h} - 1$,

then $$F_{r,h+1} > F_{r,h}, \quad (4.6)$$

i.e., the probability of failure is an *increasing* function of *h*. The following ratio validates this proposition. Indeed,

$$F_{r,h+1}/F_{r,h} = \binom{r}{h} f^{r-h} / \binom{r}{h-1} f^{r-(h-1)} = \frac{r-h+1}{fh}. \quad (4.7)$$

Proposition3: If $f<<1$,

then $$F_{r+1,h+1} > F_{r,h}. \quad (4.8)$$

Indeed, consider

$$F_{r+1,h+1} / F_{r,h} = \binom{r+1}{h} / \binom{r}{h-1} = \frac{r+1}{h} > 1. \quad (4.9)$$

The inequalities (4.4), (4.6) and (4.8) imply that

$$F_{r+1,h} < F_{r,h} < F_{r+1,h+1} < F_{r,h+1}. \quad (4.10)$$

{For illustration see the **Table1** and **Table2** in the next paragraph}.

Proposition4: Let's consider

A. $\beta := r / h$ (specific bandwidth requirement); and

B. $\rho := r - h$ (measure of redundancy).

Then the probability of failure $F(\beta, \rho)$ is a monotone *increasing* function of the bandwidth β and monotone *decreasing* function of the redundancy ρ.

Definition4: Suppose *t* is an *acceptable* probability of transmission failure (*t* is an acceptable *threshold*). In other words, if $F_{r,h} \le t$, then a *P*(*r*, *h*)-protocol is acceptable.

For example, if $F_{3,2} \le t$, then a *P*(3,2)-protocol is acceptable. Otherwise a more elaborate approach is required.

4.3. Repeated-transmission protocol

If $$f^m \le t < f^{m-1}, \quad (4.7)$$

then for redundancy the same ciphertext

Received September 23, 2008

1554-1010 $03.50 © Dynamic Publishers, Inc

$$u := E(a) \bmod n$$

is transmitted m times in the $P(m,1)$-protocol.
If a time-division multiplexing protocol [7, 12] is used, then m time frames are used to transmit each block of the ciphertext. Thus, the transmission fails only if all m attempts fail; hence the probability of failure equals $F_{m,1} := f^m$. (4.8)

5. Comparison of protocols

5.1. Probabilities of failure and bandwidth requirements

The following Table1 provides comparison of several information assurance protocols.
Basic notations in $P(r, h)$ protocol:

$F_{r,h}$ =probability of failure;

$B_{r,h}$ =bandwidth requirement per block of transmitted ciphertext.

Table1

	$P(3,2)$	$P(4,2)$	$P(5,3)$	$P(6,3)$	$P(6,4)$
$F_{r,h}$	$3f^2$	$4f^3$	$10f^3$	$15f^4$	$20f^3$
$B_{r,h}$	1.5	2	1.67	2	1.5

The protocols $P(2,1)$, $P(4,2)$, and $P(6,3)$ have the same bandwidth requirements. Yet, the latter protocol has a substantially smaller probability of failure than the previous two protocols if $f<<4/15$. Analogously, the protocols $P(3,2)$ and $P(6,4)$ have the same bandwidth requirements; yet, if $f<<3/20$, then the (6,4)-protocol fails with a significantly smaller probability than the $P(3,2)$-protocol.

Table2

r/h	**1**	**2**	**3**	**4**
3	f^3	$3f^2$	f	***
4	f^4	$4f^3$	$6f^2$	f
5	f^5	$5f^4$	$10f^3$	$10f^2$
6	f^6	$6f^5$	$15f^4$	$20f^3$

5.2. Preferability of protocols

Definition5: A protocol $P(i, j)$ is more preferable than a protocol $P(k, l)$, {and we indicate this as $P(i,j)$ f $P(k,l)$ },

if 1). $F_{ij}<F_{kl}$ (5.1)
and 2). $i/j=k/l$. (5.2)

Proposition5: If $f<<1/10$, then the following properties hold:

$$P(6,3) \text{ f } P(4,2) \text{ f } P(2,1); \quad (5.3)$$

and $$P(6,4) \text{ f } P(3,2). \quad (5.4)$$

Indeed, let's consider ratios of probabilities of failures for these protocols. Then

a). $F_{4,2}/F_{2,1}= 4f + o(f)$; {see (3.6)}

b). $F_{6,3}/F_{4,2}=15f / 4 + o(f)$; {see(3.12)}.

These ratios are substantially smaller than *one* if $f<<1/10$;

c). $F_{6,4}/F_{3,2}=20f / 3 + o(f)$,

that is smaller than one if $f<<1/10$, {see (3.4) and (3.18)}.

5.3. Illustrating example

Suppose that $f=1/100$, i.e., a communication link/channel fails in 1% of transmissions. Then the probabilities of failure in the $P(4,2)$-protocol and $P(6,3)$-protocol are respectively about 25 (*twenty five)* times and 667 (*six hundred sixty seven*) times smaller than the probability of failure of the $P(2,1)$-protocol. Furthermore,

$$F_{6,3} = 15f^4 + o(f); \ 1.5\times10^{-7}; \quad (5.5)$$

and $$F_{6,4} = 20f^3 + o(f); \ 2\times10^{-5}. \quad (5.6)$$

If an acceptable threshold of failure equals $t=10^{-6}$ {one in a *million*}, then $F_{6,3}= 1.5\times10^{-7} < t$. (5.7)

Thus the $P(6,3)$-protocol is an appropriate procedure for information assurance. However, the $P(6,4)$-protocol is not acceptable since it does not provide the information assurance if a link fails in 1% of cases.
For more details see Tables 3 & 4 and Figures 1 & 2 in the Appendix.

6. Choice of parameters of information-assurance protocol

6.1. Choice of optimal protocol

If both the probability of failure f and acceptable threshold t are specified as system performance parameters, then it is necessary to select such r and h, for which the following inequalities hold:

$$F_{r,h} \le t < F_{r-1,h} \text{ and } F_{r,h} \le t < F_{r,h+1}. \quad (6.1)$$

If several protocols satisfy the inequalities (6.1), then we select a protocol that satisfies *two* conditions:

1). It has minimal bandwidth requirement per plaintext block;

2). Recovery of the original plaintext blocks must not be too tedious; {for illustration see the 3.6. and 6.2. sections}.

Now suppose that $f=.01$ and $t=10^{-5}$.
Then several information assurance protocols can be employed to solve this problem.
For a demostration let's consider several cases:

Case *I*: $F_{3,1} = 10^{-6} \le t < F_{2,1} = 10^{-4}$;

Case *II*: $F_{4,2}=4\times10^{-6} \le t < F_{3,2}=3\times10^{-4}$;

Case *III*: $F_{5,3} = 10^{-5} = t < F_{6,4} = 2\times10^{-5}$.

Received September 23, 2008
1554-1010 $03.50 © Dynamic Publishers, Inc

Notice that the bandwidth requirement per each ciphertext block equals: in *Case I* $B_{3,1} = 3$, in Case *II* $B_{4,2} = 2$ and in Case *III* $B_{5,3} = 5/3$.

Table3: Probabilities of failures: exact and approximate values

f	**0.1**	**0.09**	**0.08**	**0.07**	**0.06**	**0.05**	**0.04**	**0.03**	**0.02**	**0.01**
E(3,2)	.028	.02284	.01818	.01401	.01037	.00725	.00467	.00265	.00118	.0003
F(3,2)	.03	.0243	.0192	.0147	.0108	.0075	.0048	.0027	.0012	.0003
E(4,2)	.0037	.00272	.00193	.0013	.00083	.00048	.00025	.00011	.00003	*insig*
F(4,2)	.004	.00292	.00205	.00137	.00086	.0005	.00026	.00011	.00003	*insig*
E(5,3)	.00856	.00634	.00453	.00308	.00197	.00116	.0006	.00026	.00008	.00001
F(5,3)	.01	.00729	.00512	.00343	.00216	.00125	.00064	.00027	.00008	.00001

Table 4: Probabilities of failure: ratios $E(r,h)/F(r,h)$

f	**0.1**	**0.09**	**0.08**	**0.07**	**0.06**	**0.05**	**0.04**	**0.03**	**0.02**	**0.01**
S(3,2)	.93333	.94	.94667	.95333	.96	.96667	.97333	.98	.98667	.99333
S(4,2)	.925	.9325	.94	.9475	.955	.9625	.97	.9775	.985	.9925
S(5,3)	.856	.86986	.88384	.89794	.91216	.9265	.94096	.95554	.97024	.98506

Fig1: Probabilities of failure: exact and approximate values

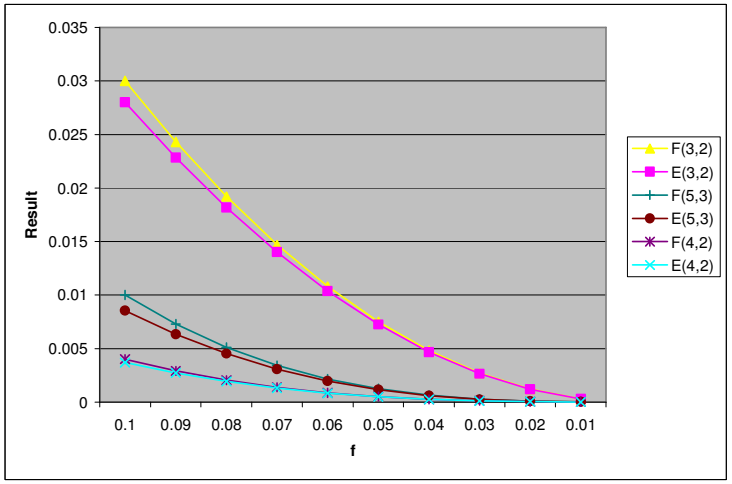
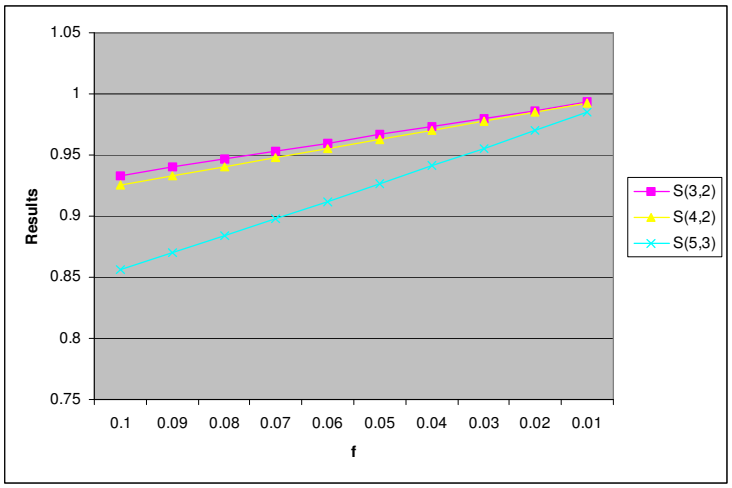


Fig2: Probabilities of failure: ratios $E(r,h)/F(r,h)$



Received September 23, 2008
1554-1010 $03.50 © Dynamic Publishers, Inc

Hence, the $P(5,3)$-protocol is 80% faster than the $P(3,1)$-protocol and 20% faster than the $P(4,2)$-protocol.

To employ the $P(5,3)$-protocol for information assurance and secure transmission we need to select *five* linearly-independent combinations:

$$\left\{\sum_{i=1}^{3} g_{i1}a_i, \sum_{i=1}^{3} g_{i2}a_i, ..., \sum_{i=1}^{3} g_{i5}a_i\right\} \qquad (6.2)$$

These combinations must be selected in such a way that the recovery of a_1, a_2 and a_3 will be as simple as possible.

6.2. Parametric analysis of combinations

Let us consider five combinations with one parameter w:

$$\{A, B, C, D, E\}:= \{a-b, 2a+b, a+wb+c, b+2c, b-c\}. \qquad (6.3)$$

If the parameter w=2, then there are ten combinations of transmission; and it is necessary that each combination must be easy solvable. Let consider some of them and show how the original plaintext blocks *a, b* and *c* can be recovered:

Case *{A, B, C}*: Then $a:=(A+B)/3$

$$b := a - A; \quad c := C - a - 2b; \qquad (6.4)$$

Case *{A, B, D}*: Then $a := (A + B)/3;$

$$b := a - A; \quad c := (D - b)/2; \qquad (6.5)$$

Case *{A, B, E}*: Then $a := (A + B)/3;$

$$b := a - A; \quad c := b - E; \qquad (6.6)$$

Case *{A, C, D}*: Then $b := [2(C - A) - D]/5;$

$$c := (D - b)/2; \; a:=A+b; \qquad (6.7)$$

Case *{B, C, D}*: Then $a := (B - 2C + D)/4;$

$$b := B - 2a; \quad c := (D - b)/2; \qquad (6.8)$$

Comment: We leave to a reader of this paper to verify ease of recovery for the remaining five cases:

$\{A, C, E\}$; $\{A, D, E\}$;$\{B, C, E\}$; $\{B, D, E\}$ and $\{C, D, E\}$.

Suppose that in the combination C the parameter $w = -2$. Then it is easy to verify that in the case $\{A, C, E\}$ it is impossible to recover the plaintext blocks *a*, *b* and *c*; analogously, if in the combination *C* the parameter $w = 1$, then the recovery of the plaintext blocks *a*, *b* and *c* in the case $\{B, C, D\}$ is impossible.

Overall analysis shows that in (6.3) all integer values of w are acceptable with two exceptions: $w \neq -2$ and $w \neq 1$. And finally, if $w = 1/2$, then in the case $\{A, C, D\}$ the plaintext blocks *a, b* and *c* are not recoverable because not all combinations in (6.3) are linearly independent.

7. Adaptive vs. non-adaptive transmission

More reliable protocols of transmission can be introduced if adaptability is appropriate, which is not always the case. Indeed, there are circumstances, in which only one-way communication is feasible: communication with a deep-space craft whether it is man controlled or machine controlled; clandestine communication, where a receiver needs to keep "radio" silence; weapon-control protocol, where real-time control requirements combined with possibility of high-level noise do not allow time for response/ACK and adjustment.

8. Conclusions

Several protocols of information assurance are considered in this paper and their efficiencies are analyzed in several examples. It is also demonstrated how to select an optimal protocol that takes into account reliability of transmission channels, satisfies acceptable requirements on information assurance, and allows easy recovery of the original information.

Acknowledgements

I express my appreciation to R. Rubino for comments that improved the quality of this paper and my gratitude to K. Skov for computer assistance in preparation of graphics.

References

[1] N. Falby, J. Fulp, P. Clark, R. Cote, C. Irvine, G. Dinolt, T. Levin, M. Rose, and D. Shifflett, "*Information assurance capacity building: A case study,*" Proc. 2004 IEEE Workshop on Information Assurance, U.S. Military Academy, June, 2004, 31-36.

[2] V. Gorodetsky, V. Skormin, and L. Popyack (Eds.), *Information Assurance in Computer Networks: Methods, Models, and Architecture for Network Security*, St. Petersburg, Springer, 2001.

[3] J. Hamill, R. Deckro, and J. Kloeber, "*Evaluating information assurance strategies*," in Decision Support Systems, Vol. 39, Issue 3 (May 2005), 463-484.

[4] A. Leon-Garcia, I. Widjaja, *Communication Networks*, McGraw Hill, 2000.

[5] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[6] NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

[7] M. Rabin, "*Digitized signatures and public-key functions as intractable as Factorization*," MIT/LCS Technical Report, TR-212 (1979).

[8] R. L. Rivest, A. Shamir and L.M. Adleman, "*A method for obtaining digital signature and public-key*

Received September 23, 2008

1554-1010 $03.50 © Dynamic Publishers, Inc

cryptosystems," Communication of ACM, 21, (1978), 120-126.

[9] M. Schwartz, *Broadband Integrated Networks*, Prentice Hall, 1996.

[10] Boris S. Verkhovsky, "*Entanglements of plaintext streams and cubic roots of integers for network security*," Advances in Technology and Intelligent Information Systems, Vol. IX, July, 2008, IIAS, 90-93.

[11] Boris S. Verkhovsky, "*Information assurance and secure streaming algorithms based on cubic roots of integers*," in *Fifth Intern. Conf. on Information Technology*: *New Generations* (*ITNG*-2008), IEEE Computer Society: Las Vegas, Nevada, USA, 910-916.

[12] Boris S. Verkhovsky, "*Fast algorithm for modular multiplicative inverse,*" Advances in Computer Cybern., Vol. VII, 2000, 11-15.

[13] Boris S. Verkhovsky, "*Enhanced Euclid algorithm for modular multiplicative inverse and its complexity*", Advances in Computer Cybernetics, Vol. VI, 1999, 51-57.

[14] Boris S. Verkhovsky, "*Control protocols providing information assurance in telecommunication networks,*" Oct. 2008, {submitted for publication}.

Dr. Boris S. Verkhovsky is a Professor of Computer Science at the New Jersey Institute of Technology.. He received his PhD in Computer Science jointly from Latvia State University and from the Academy of Sciences of the USSR (Central Institute of Mathematics and Economics). From his prior affiliations at the Moscow Scientific Research Institute of Computers, Princeton University, IBM Thomas J. Watson Research Center, Bell Laboratories and since 1986 at the NJIT, he acquired vast research interests and experience in cryptography, communication security, large-scale systems optimal design & control, operations research, optimization and algorithms design. He published more than two hundred papers. For the last twenty years the research activity of Dr. Verkhovsky is in design and analysis of cryptosystems.

Professor Verkhovsky is a recipient of numerous awards including the USSR Ministry of Radio-Electronics Award; the Academy of Sciences of the USSR Award; Alvin Johnson Award; Millennium Award and Medal of Excellence. Verkhovsky was Wallace Eckert Scientist at the IBM Research, Associate Professor at Princeton University, Member of Technical Staff at Bell Labs and held Charles Dana Endowed Chair Professorship. In 2003 Dr. Verkhovsky received Blasé Pascal Medal in Computer Science and was elected as a Fellow of European Academy of Science (EAS). He is listed in Marquis *Who'sWho in America*.

Received September 23, 2008 1554-1010 $03.50 © Dynamic Publishers, Inc